UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/216,519	12/18/98	KERR	D 112025-0112

WM31/1024

CHARLES J BARBAS
CESARI AND MCKENNA
30 ROWES WHARF
BOSTON MA 02110

EXAMINER	
NEWTON, G	
ART UNIT	PAPER NUMBER
2132	8

DATE MAILED: 10/24/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 09/216,519	Applicant(s) KERR ET AL.	
	Examiner Gregory A Newton	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *18 December 1998* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Specification

Copending US Patent Application serial number 112025-77 disclosed in page 10 of application specification is not found through available reference channels.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2. Claims **1-6, 10-12, 15**, are rejected under 35 U.S.C. **102(e)** as being anticipated by **Narad et al** (US 6,157,955).

Claim 1 recites an apparatus for tightly coupling hardware data encryption functions with software based protocol processing within a pipelined processor of a programmable processing engine in a network switch. Refer to Narad et al reference of note for such disclosures. For tightly coupling hardware data encryption with software based protocol decode processing, refer to column 4, top line, lines 36-37, lines 46-47, line 54. For disclosures of pipelining see column 3, lines 55-60. For disclosures of network switching see column 3, section 3, Switches and Routers. For illustration of

and encryption execution unit within pipelined processor see figure 2, item 112. For software and hardware interface enabling encryption execution to efficiently cooperate with processing resources see e.g. ABSTRACT.

Claim 2 recites apparatus of claim **1** with further limitations of the encryption execution unit being an encryption tightly coupled state machine unit that is selectively invoked within the pipelined processor. Refer to Narad et al reference; for tightly coupled encryption unit refer to top of column 4. For encryption unit being a state machine refer e.g. to ABSTRACT. For multiple/overlapping functional cryptographic ability (TCSM, given in specification page 5) refer to illustration in figure 3, items 246 and 202. Selective invocation of cryptographic unit within pipelined processor may be found e.g. column 6, last paragraph, and top of column 7.

Claim 3 recites the apparatus of claim **2** with further limitations. For disclosures of instruction set coding for encryption refer to column 8, last line, and column 9, lines 5-10. Selective access of the cryptographic unit within pipelined processor may be found e.g. in column6, last paragraph, and top of column 7.

Claim 4 recites the apparatus of claim **3** with further limitations of a plurality of busses in the pipelined processor wherein the encryption unit utilizes internal buses in response to encryption processing operation code. Refer to Narad et al figure 1, and discussions thereon in column 6, penultimate paragraph, and teachings concerning preferred embodiment of a Policy Engine, column 6, last paragraph. Pipelined architecture is pointed out in column 6, line 61. Buses are illustrated in figure 1 as wide arrows, which carry data, control commands, etc., which interlink the Application

Processor (item 4) and the Policy Engine (PE, item 6). The PE encryption unit operation codes communicating with the buses depicted in figure 1 are discussed e.g. top of column 7, lines 1-6, as well as column 16, lines 5-10..

Claim 5 recites the apparatus of claim **4** with further limitations. For core processor see column 14, e.g. lines 5-9 in the section on processor interfaces. For multi-stage pipelined architecture see e.g. column 3, lines 55-60. For pipeline architecture including instruction fetch, decode, execute, memory writing stages, refer to figure 14 and column 40, lines 59-66.

Claim 6 recites apparatus of claim **5** with further limitations of the pipelined processor (described TMC in claim 5) including arithmetic logic unit, at least one internal register, an instruction fetch and decode unit, and the encryption unit organized as a data path. For pipelined processor including an arithmetic logic unit and internal register, see column 37, paragraph line 45. For instruction fetch and decode, see figure 14. For the (tightly coupled) encryption unit organized as a data path see figure 2, item 112, or see column 30, lines 46-47.

Claims 10-12 are method claims corresponding to the apparatus claims **1, 3, 4**, respectively, and are rejected in view of the same prior art of record and in accordance with the same rationale.

Claim 15 recites the method of claim **12** with further limitations. For the encryption unit being tightly coupled state machine refer to e.g. top of column 4. For disclosures of initializing the encryption unit in response to execution of a first instruction that defines the form of operation to be performed see e.g. column 7, lines 1-2.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims **7-9, 13-14, and 16-19,** are rejected under 35 U.S.C. **103(a)** as being unpatentable over **Narad et al** (US 6,157,955) in view of **official notice**.

Claim 7 recites the apparatus of claim **5** with further limitations of the (tightly coupled) encryption unit comprising a Data Encryption Standard (DES) functional component cooperatively coupled to a sub key generation functional component. For key management (generation) refer to **Narad et al**, e.g. column 7, line 6.

Narad et al are silent with respect to Data Encryption Standard. However, examiner takes official notice that DES would be an obvious option for cryptographic functions, as implied by the word "standard".

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with the encryption function of Data Encryption Standard in order to choose a cryptographic function for the tightly coupled encryption facilities. One of ordinary skill in the art would have been motivated to do this because DES is a standard set forth by cryptology experts.

Claim 8 recites the apparatus of claim **5** with further limitations of the DES cryptographic function comprising state machine hardware used to execute each round of a DES function. For **Narad** device comprising state machine hardware with encryption function see e.g. ABSTRACT, and figures 2 and 3.

Narad et al are silent with respect to Data Encryption Standard being implemented on hardware illustrated in figures 2 and 3 and discussed throughout reference. However, examiner takes official notice that implementing the Data Encryption Standard into the cryptographic hardware illustrated in figures 2 and 3 of Narad et al would have been an obvious choice for one of ordinary skill in the art.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with the Data Encryption Standard in order to provide encryption functionality into the hardware crypto modules illustrated in figures 2 and 3 of Narad et al. One of ordinary skill in the art would have been motivated to do this by referring to Narad et al, e.g. bottom three paragraphs of column 3, and top 3 paragraphs of column 4, where motivation is provided for implementation of specialized encryption hardware in order to accelerate applications. Implementing the Data Encryption Standard would have been an obvious choice, implied by the term "standard".

Claim 9 recites the apparatus of claim **7** with further limitations of the key generation for each round of the Data Encryption Standard function being generated by hardware componentry. Keys for cryptographic hardware are discussed in **Narad et al** e.g. column 7, line 6.

Narad et al are silent with respect to explicit disclosure of hardware supplying keys for Data Encryption Standard function rounds. However, examiner takes official notice that the Data Encryption Standard would have been an obvious function for the cryptographic modules of Narad et al which are illustrated in e.g. figures 2 and 3. This is implied by the term "standard" in the Data Encryption Standard.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with the Data Encryption Standard in order to generate keys for DES rounds from hardware arrangements. One of ordinary skill in the art would have been motivated to do this by referring to Narad et al e.g. column 3, lines 60-65, and top of column 4, where motivation is explicitly set forth for optimizing the cryptographic functions of the Narad device by implementation of specialized hardware for encryption, (e.g. supplying keys for DES rounds).

Claim 13 recites the method of claim **12** with further limitations. For plaintext stored at the network switch see **Narad et al**, e.g. column 7, lines 25-30. For cryptographic functions operating on plaintext stored at a switch see e.g. column3, lines 13-14, where it is said that segments are visible to the switches, i.e. including the cryptographic segment.

Narad et al are silent with respect to explicitly teaching the processing of protocols contained in the plaintext for determining an appropriate encryption algorithm. However, for implicit teachings regarding protocols for choosing what operations to

perform, i.e. which encryption algorithm, see column 27, lines 4-7. See also column 16, esp. lines 16-20.

Narad et al are silent with respect to explicit disclosures of determining the appropriate encryption algorithm and immediately fetching initial cryptographic keys. However, for implicit but clear teachings of determining cryptographic operations and key management directed to one of ordinary skill in the art, see column 27, line 5.

Narad et al are silent with respect to explicit referrals to providing keys to the crypto unit after fetching crypto keys, however, see column 27, line 5, for such teachings directed to one of ordinary skill in the art.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with the steps above taught implicitly by Narad et al in order to enable encryption by available functions as well as key procurement and management. One of ordinary skill in the art would have been motivated to do this for enablement of encryption in a processing engine such as Narad's, which relies on teachings of applied cryptography used by one of ordinary skill in the art, and which need not be disclosed in the scope of Narad's teachings, as discussed in column 3, lines 50-52.

Claim 14 recites the method of claim **13** with further limitations. For high performance busses in the pipelined processing engine, see **Narad et al** e.g. figure 1, where control code, policy modifications, data, etc, travel on these busses (wide arrows).

Narad et al are silent with respect to explicit disclosures of accessing internal busses through integrated interface to simultaneously load an encryption key and store a previous result. However, see column 16, lines 5-10, for motivation. For motivation to configure simultaneous and tightly coupled executions such as loading keys while storing results see e.g. column 4, lines 1-2. See especially column 7, lines 4-6, for motivation to accelerate cryptographic processing by simultaneous processing, where auxiliary cryptographic processors are discussed.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad with simultaneous cryptographic processing in order to load keys while storing previous results. One of ordinary skill in the art would have been motivated to do this because to make simultaneous is well known to modify prior art.

Claim 16 recites the method of claim **15** with further limitations. For coupling optional cryptographic processors see **Narad et al**, column 7 lines 4-6.

Narad et al are silent with respect to explicit disclosures of a DES processor coupled to a key generation unit. However, see column 7, lines 4-6, for coupling cryptographic processes. See further column 7, lines 5-6, for motivation concerning key management, i.e., key generation.

Narad et al are silent with respect to explicit disclosures of initializing a DES function by decoding a first portion of the first instruction and decoding a second portion of the first instruction to initialize DES crypto key. However, refer to figure 14 for illustration of decoding combined instructions. Figure 14 is generic to Narad et al

processing engines, e.g. crypto processors. For implicit motivation for decoding such combined instruction codes (e.g. for key generation) as illustrated in figure 14, item 1304, see e.g. column 7, lines 5-6.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with Data Encryption Standard crypto function order to provide Narad's cryptographic processing engine with a standard encryption function such as DES. One of ordinary skill in the art would have been motivated to do this because the Data Encryption Standard is well known in the art as encryption function, as is implied by the term "Standard".

Claim 17 recites the method of claim **16** with further limitations. For disclosures of instruction set coding specially for encryption refer to **Narad et al**, column 8, last line, and column 9, lines 5-10. For fetching instructions see e.g. figure 14, item 1302. For operations such as fetching keys from memory, see section titled Crypto Command Queue and Communication Rings at bottom of column 26, and further top of column 27, esp. line 5. Auxiliary crypto processors are illustrated e.g. figure 3, items 246 and 202.

Narad et al are silent with respect to an explicit disclosure reciting a second instruction having a micro-opcode field containing a native encryption opcode that specifies loading an initial key from a memory into the sub-key generation functional component of the encryption unit. However, all such features of key procurement and management are summarized in Narad e.g. column 7, lines 1-5, and column 3 lines 50-55.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad with such explicit key management features in order to allow for encryption as taught in Narad's processing engine. One of ordinary skill in the art would have been motivated to do this because Narad's teachings on tightly coupled processing engine embodiments are inclusive of key management, and are directed to one of ordinary skill in the art to include coding instruction for key procurement from memory as in column 27, lines 4-7.

Claim 18 recites the method of claim **17** with further limitations of Data Encryption Standard implementations. However, DES implementation is well known in the art, as implied by the term "standard". Refer to **Narad et al** for teachings directed to one of ordinary skill in the art. For teachings on cryptographic functions, refer to column 7, lines 1-5.

Narad et al are silent with respect to explicitly implementing the DES encryption algorithm into their tightly coupled processing engine. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with encryption performed by the DES algorithm in order to implement an encryption algorithm for the tightly coupled processing engine of Narad et al. One of ordinary skill in the art would have been motivated to do this because DES is well known in the art as an encryption algorithm, as is implied by the term "standard".

For teachings regarding machine operation code instructions directing the encryption procedure, refer e.g. to column 27, lines 1-7. Narad et al are silent with respect to execution of a third instruction that initiates encryption by a DES function.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with a third instruction with machine code initiating encryption by DES function in order to proceed with encryption. One of ordinary skill in the art would have been motivated to do this by referring to Narad et al e.g. top of column 7, where teachings directed to one of ordinary skill in the art are disclosed including encryption, key procurement and management, etc.

For registers coupled to the cryptographic functions unit refer e.g. to column 16, section 7, titled Crypto Control. Narad et al are silent with respect to explicitly describing a register for DES, but the scope of Narad et al's tightly coupled processing engine refers encryption implementation details to one of ordinary skill in the art.

Claim 19 recites the method of claim **18** with further limitations. For teachings regarding machine code instructions for directing encrypted results, refer to **Narad et al** bottom of column 26 and top of column 27, and also see column 16, section 7, titled Crypto Control.

Narad et al are silent with respect to explicit teachings of a fourth instruction to store the ciphertext results contained in the internal register to a location in the memory. However, teachings of Narad et al directed to one of ordinary skill in the art would have motivated one to employ such connections. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with a fourth instruction to store ciphertext contained in the internal register to a location in the memory in order to provide connections to the

cryptographic function of the Narad et al tightly coupled processing engine. One of ordinary skill in the art would have been motivated to do this to provide connection to the encryption units.

5. Claim **20** isrejected under 35 U.S.C. **103(a)** as being unpatentable over **Narad et al** (US 6,157,955) in view of **Key et al** (US 6,173,386).

Claim 20 recites a programmable processing engine of a network switch with input and output buffers buffering an array of rows and columns of processing elements. For tightly coupled crypto processor with integrated hardware and software interface allowing efficient encryption, see **Narad et al**, e.g. ABSTRACT. Narad et al are silent with respect to explicit disclosures of such an array, although references to buffer/processor connectivity are found throughout, e.g. figure 2. However, see **Key et al** e.g. figure 3 for such an array.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Narad et al with the teachings of Key et al in order to allow pipeline connectivity. One of ordinary skill in the art would have been motivated to do this in order to implement a specific embodiment feature of the Narad et al tightly coupled processing engine, discussed in Narad et al e.g. column 3, SUMMARY, and top of column 4.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory A Newton whose telephone number is 703-305-1373. The examiner can normally be reached on 9-6 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on 703-305-9595. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

gn

gn
October 8, 2001

PHUNG M. CHUNG
PRIMARY EXAMINER